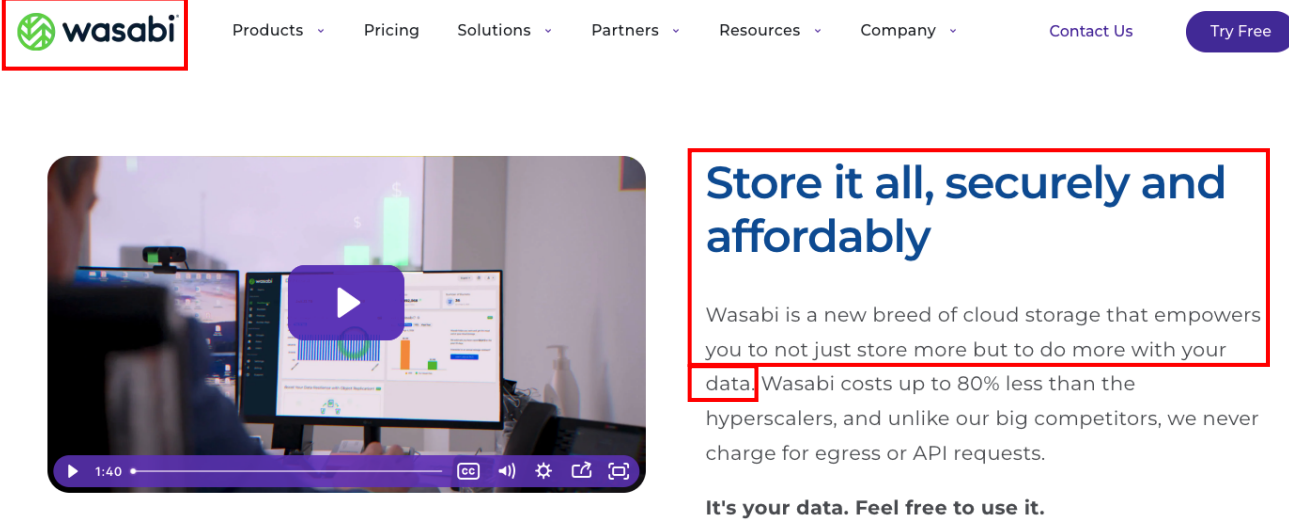


# EXHIBIT B

**U.S. Patent No. US 8,856,221 v. Wasabi Technologies LLC**

## 1. Claim Chart

Claim	Analysis
<p>[7.P] A method for storing media content and delivering requested media content to a consumer device, the method comprising:</p>	<p>Wasabi Technologies LLC (“Company”) performs and/or induces others to perform a method for storing media content and delivering requested media content to a consumer device.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Company provides a cloud storage solution that enables users to store various types of data, including text, photos, and videos (“media content”), on the Wasabi Cloud. Additionally, Wasabi integrates NirvaShare, a third-party file-sharing and access management solution that allows users to securely manage, share, view (“delivering requested media content”), and download (“storing media content”) files directly from the Wasabi Cloud via a dedicated user interface on their device (“consumer device”).</p>  <p>Source: <a href="https://wasabi.com/cloud-object-storage">https://wasabi.com/cloud-object-storage</a></p>

## WASABI HOT CLOUD STORAGE (Console)

Updated on 06 Nov 2024 · 3 Minutes to read

Print Share PDF



Wasabi Hot Cloud Storage is a cloud-based object storage service for a broad range of applications and use cases.

Wasabi Hot Cloud Storage provides a simple web service interface that is 100% Amazon S3 bit-compatible. Wasabi can store and retrieve any amount of data at any time from anywhere on the web. Because Wasabi is highly scalable and you only pay for what you use, developers can start small and grow their applications as they wish, with no compromise to performance or reliability.

Wasabi allows you to store virtually any kind of data in any format. For more detail, review Wasabi's [Terms of Use Agreement](#).

Wasabi Hot Cloud Storage is designed for individuals and organizations that require a high-performance, reliable, and secure data storage infrastructure at minimal cost. The following guides will help you get started and delve deeper into Wasabi features. Refer to the information below these lists for general insight into Wasabi Hot Cloud Storage.

Source: <https://docs.wasabi.com/v1/docs/wasabi-cloud-storage-console-1>



[Get Started](#) [White Papers](#)

## Secure File Sharing & Access Management Solution For Your Object Storage

A self hosted server for secure file Sharing and Collaboration from Object Storages such as AWS S3, Azure Blob, GCP, DigitalOcean Spaces, MinIO and many more in a most simplified way.

Supports a variety of authentication options while sharing files with users such as SSO with Multi-Factor, Basic, Form and OTP based with granular access control.

Source: <https://nirvashare.com/>

### ▲ [What Cloud Storage providers are supported by NirvaShare?](#)

NirvaShare supports prominent Cloud storage providers like AWS S3, Google Cloud, Azure Blob, Digital Ocean Spaces, MinIO, Backblaze B2, Oracle, Linode, Wasabi and many others.

Source: <https://nirvashare.com/faqs/>

# NirvaShare With Wasabi

Updated on 20 Jun 2024 · 2 Minutes to read

Print Share PDF

## How do I use NirvaShare with Wasabi?

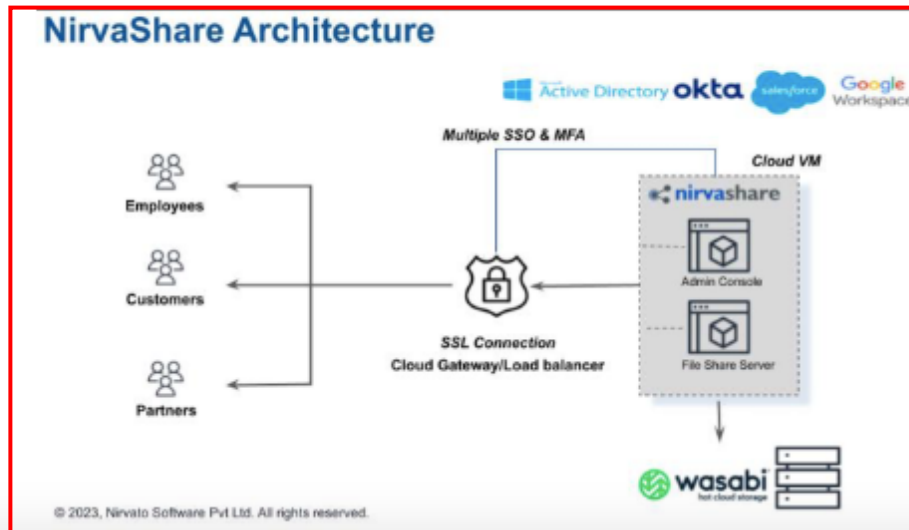
Wasabi's object storage has been validated to be used with NirvaShare.

[NirvaShare](#) is a Secure File Sharing & Access Management Solution for Wasabi's object storage. It provides an easy SSO integration with identity providers like Active Directory, Okta, etc.

## 1. Prerequisites

- NirvaShare version 2.4.0 and above is installed.
- An active Wasabi cloud storage account.

## 2. Architecture Diagram



Source: <https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi>

## Storing Objects in a Bucket

media content

You can store objects in a bucket in Wasabi. An object can be any type of file—text, photo, video, etc. See [Step 2 in Getting Started: Working with a Bucket](#).

Source: <https://docs.wasabi.com/docs/storing-objects-in-a-bucket> (annotated)

### About




Enterprise Secure File Sharing of Cloud Storage such as AWS S3, Azure, Wasabi, Digital Ocean Space, MinIO, and Linode is simplified now!

Securely share and collaborate any folder or file with external identities such as customers, partners, vendors, etc with security and fine access control including internal identities like employees.

Supports variety of authentication options such as Federated SSO (SAML2), Basic, Form and OTP based. Integrates with identity providers like GSuite, Active Directory, Salesforce, Okta, WordPress, and AWS SSO.

NirvaShare is an enterprise secure file sharing software featuring document copy protect, branding, digital signature, IP white listing, auditing, etc.

Source: [https://www.youtube.com/channel/UCP8znBILQ0b\\_2ixAak\\_iDcw](https://www.youtube.com/channel/UCP8znBILQ0b_2ixAak_iDcw)

	<div data-bbox="415 267 638 306"></div> <div data-bbox="1087 276 1793 303"><a href="#">Get Started</a> <a href="#">White Papers</a> <a href="#">Case Studies</a> <a href="#">Pricing</a> <a href="#">Request a Demo</a></div> <div data-bbox="632 443 1480 482"><h2>How to Share File/Folder and Manage Access to Wasabi Storage</h2></div> <div data-bbox="632 490 823 519"><a href="#">/ Blogs, Installations</a></div> <div data-bbox="640 586 1661 714"><h1>How to Share File/Folder and Manage Access to Wasabi Storage</h1></div> <div data-bbox="640 755 1778 894"><p>Wasabi is a cloud platform that provides object storage space for companies to store a large number of files. The biggest challenge when it comes to object storages is with respect to file or folder sharing. NirvaShare, a secure file sharing platform addresses this challenge effectively. In this document, we will discuss the method to configure and share files from Wasabi storage using NirvaShare file sharing and share file/folder efficiently with users.</p></div> <div data-bbox="394 919 1623 959"><p>Source: <a href="https://nirvashare.com/how-to-share-file-folder-and-manage-access-to-wasabi-storage/">https://nirvashare.com/how-to-share-file-folder-and-manage-access-to-wasabi-storage/</a></p></div>
--	---



## Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: <https://nirvashare.com/white-papers/>

Setup Guide 3

CREATE NEW SHARE

Path: elasticbeanstalk-ap-south-1-100674486567/test folder/

Basic InfoPermissionsAuthenticationDuration

Access Levels ?

☒ Can Delete ☒ Can Upload ☒ Can Create Folder ☒ Can Download ☐ Add Digital Signature

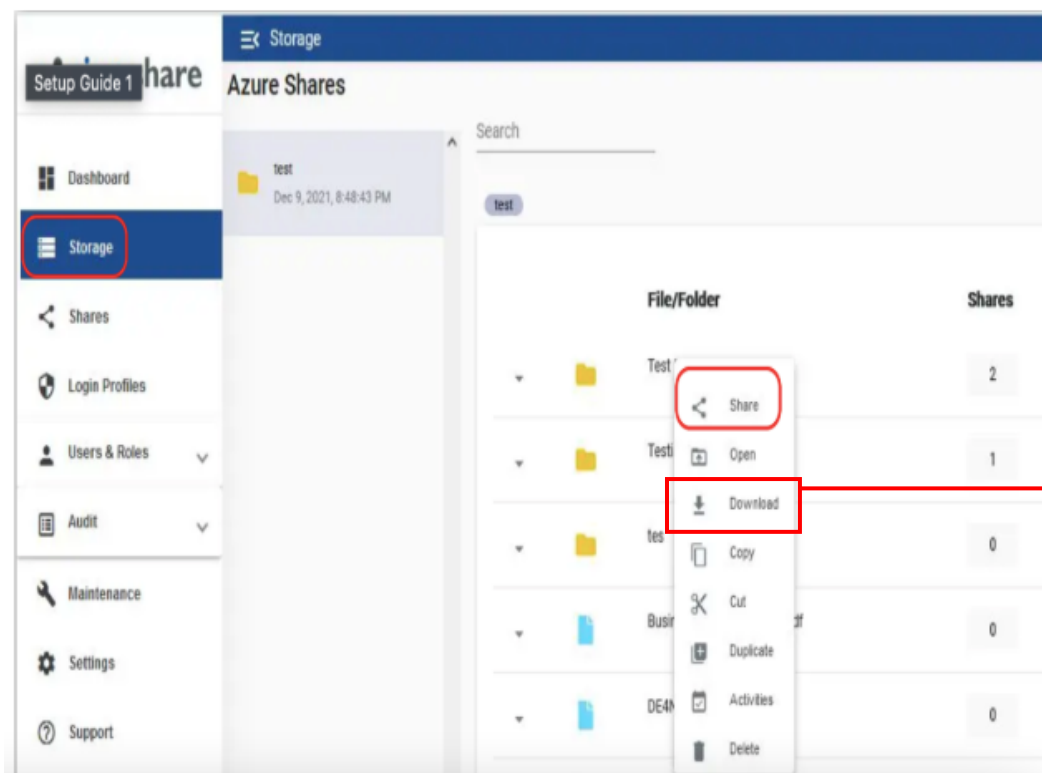
☐ View with Copy Protect — delivering requested media content

Source: <https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi> (annotated)

## 5. File/Folder Sharing with Username and Password Authentication

After the Wasabi bucket is added, the next step is to browse the storage file/folder and share it with users. Follow the steps below to create a **Share** for a folder with simple Form-based authentication.

**5.1 Click on the "Storage" tab on the left menu.** The storage files will be listed here, browse through any file or folder, and select "Share" by right clicking on it. Then click "Create New Share" to create a new file share.



storing media content

Source: <https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi> (annotated)

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

<p>[7.1] receiving a request message including media data indicating requested media content and a consumer device identifier correspondin g to the consumer device;</p>	<p>Company performs and/or induces others to perform the step of receiving a request message including media data indicating requested media content and a consumer device identifier corresponding to the consumer device.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Wasabi integrates NirvaShare for secure file sharing and access management from the Wasabi Cloud. NirvaShare allows file owners to share files via a URL and apply authentication measures, such as basic authentication, to control access. When a file owner shares the URL with a user, the user must authenticate using a username and password (“a consumer device identifier”) upon accessing the link. Therefore, upon information and belief, when the user opens the shared URL, a request is generated containing authentication data and information about the shared file (“media data indicating requested media content”).</p>
--	--

## NirvaShare With Wasabi

Updated on 20 Jun 2024 · 2 Minutes to read

Print Share PDF

### How do I use NirvaShare with Wasabi?

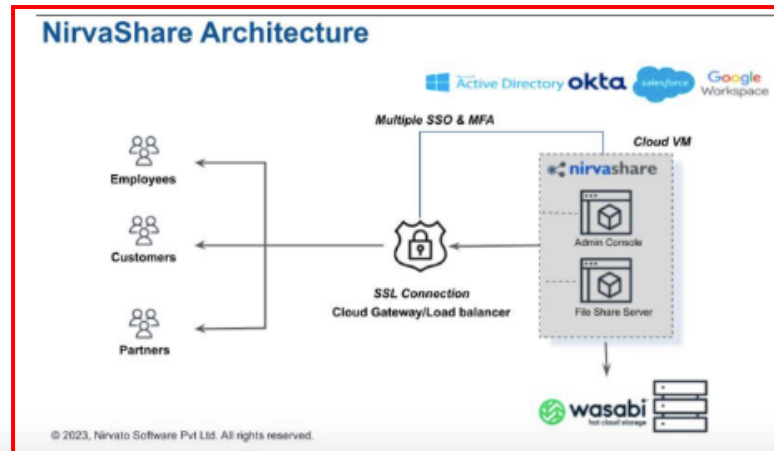
Wasabi's object storage has been validated to be used with NirvaShare.

[NirvaShare](#) is a Secure File Sharing & Access Management Solution for Wasabi's object storage. It provides an easy SSO integration with identity providers like Active Directory, Okta, etc.

### 1. Prerequisites

- NirvaShare version 2.4.0 and above is installed.
- An active Wasabi cloud storage account.

### 2. Architecture Diagram



Source: <https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi>

## Sharing A File Or Folder

Sharing a File/Folder from object storage with users can be done by creating a Share and granting restrictive access to it. In this document, we will walk you through creating a new Share, setting access permissions, and sharing the same with users.

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>

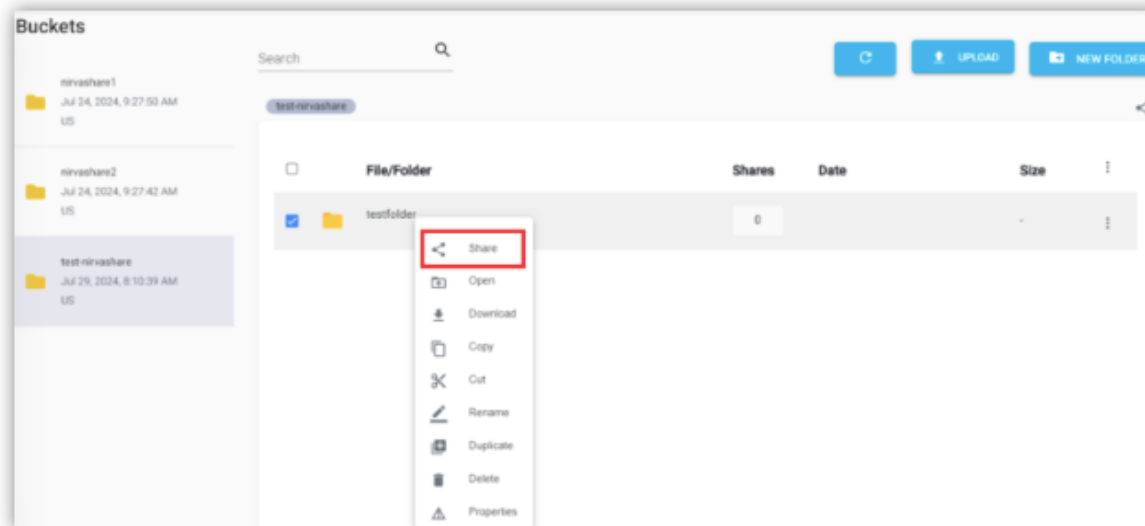
### ▲ Can we share any file or folder?

Yes, any folder or single file can be shared to users. Each share can have access rights.

Source: <https://nirvashare.com/faqs/>

## New Share

From the NirvaShare Admin Console, click on the **Storage** tab from the left menu and browse through the files. Select any file or folder and right-click to get the context menu. Select **Share** to create a new share.



Provide a name and description for the **Share**. Before clicking on **Create Share**, move to the next tabs to set other configurations.

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>

## Authentication

Authentication can be set for the shared files. When users access this shared URL, authentication will be performed depending on the type that was set here. Supported authentication types are Basic, Form (single user), Form (multi users), OTP, FTPS and External IDP integration.

The screenshot shows a web interface for configuring authentication settings. It features a tabbed navigation system with four tabs: 'Basic Info', 'Permissions', 'Authentication' (which is currently selected), and 'Duration'. Under the 'Authentication' tab, there is a list of radio button options: 'None (No Access)', 'Public Access', 'Basic Authentication (Single User)', 'Form Based (Single User)', 'Form Based (Multiple Access Users)', 'External Single Sign-On (SSO)', 'One-time Password (OTP)' (which is selected), and 'FTPS'. Below these options, there is a dropdown menu labeled 'Select Existing Login Profile \*' with 'otp' selected, and a 'New' button. At the bottom right of the interface, there are two buttons: 'CANCEL' and 'CREATE SHARE'.

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>



	<p><b>Basic Authentication</b> – It provides old method of browser based username password way of authentication. The credentials are passed with http header after encoding.</p> <p>A consumer device identifier corresponding to the consumer device</p> <p>Source: <a href="https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/">https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/</a> (annotated)</p> <h3>Verification</h3> <ul style="list-style-type: none"> <li>• For verifying the above procedure pertaining to file sharing, Copy the <b>Shareable Link</b> from the shares.</li> <li>• Open the link in browser tab. This will redirect to Form based authentication.</li> <li>• Once the authentication is effective, you should be able to access <b>Shares</b> assigned to the login profile.</li> <li>• This link can be emailed or shared with your users.</li> </ul> <p>Source: <a href="https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/">https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/</a></p> <p>Further, to the extent this element is performed at least in part by Defendant’s software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.</p>
[7.2] determining whether the consumer device identifier corresponds to a registered consumer	<p>Company performs and/or induces others to perform the step of determining whether the consumer device identifier corresponds to a registered consumer device.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, to access the shared URL, NirvaShare requires users to authenticate according to the authentication method set by the file owner, such as basic authentication. Therefore, it would be apparent to a person having ordinary skills in the art that when the recipient of the shared files completes authentication, NirvaShare verifies the user (“determining whether the consumer device identifier corresponds to a registered consumer device”) based on the provided username and password (“the consumer device identifier”).</p>

<p>device; and; if it is determined that the consumer device identifier corresponds to the registered consumer device, then:</p>	<div data-bbox="422 326 1698 453" style="border: 1px solid red; padding: 5px;"> <p><b>Basic Authentication</b> – It provides old method of browser based username password way of authentication. The credentials are passed with http header after encoding.</p> </div> <p style="text-align: center; color: red;">the consumer device identifier</p> <p>Source: <a href="https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/">https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/</a> (annotated)</p> <div data-bbox="405 594 1801 914" style="border: 1px solid red; padding: 5px;"> <p><b>Verification</b> — determining whether the consumer device identifier corresponds to a registered consumer device</p> <ul style="list-style-type: none"> <li>• For verifying the above procedure pertaining to file sharing, Copy the <b>Shareable Link</b> from the shares.</li> <li>• Open the link in browser tab. This will redirect to Form based authentication.</li> <li>• Once the authentication is effective, you should be able to access <b>Shares</b> assigned to the login profile.</li> <li>• This link can be emailed or shared with your users.</li> </ul> </div> <p>Source: <a href="https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/">https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/</a> (annotated)</p> <p>Further, to the extent this element is performed at least in part by Defendant’s software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.</p>
<p>[7.3] determining, whether the request message is one of a storage request message and</p>	<p>Company performs and/or induces others to perform the step of determining, whether the request message is one of a storage request message and a content request message.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, after signing in, when the user accesses the shared URL, NirvaShare displays the shared files. Additionally, NirvaShare allows the file owner to define access-level permissions, such as ‘can download folder’ and ‘view with copy protect’. Therefore, it would be apparent to a person having ordinary skills in the art that once the files are shared with these access levels, NirvaShare provides the user with options to view or download them. If the user selects the view option (“a content request message”), NirvaShare opens and displays the file, while if the user selects the download</p>

<p>a content request message; and;</p>	<p>option (“a storage request message”), NirvaShare downloads the file for the user. Hence, NirvaShare performs the step of determining, whether the request message is one of a storage request message and a content request message.</p> <h2>Access Levels</h2> <p>Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.</p> <p>Source: <a href="https://nirvashare.com/white-papers/">https://nirvashare.com/white-papers/</a></p>
--	--

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

The screenshot displays the 'Permissions' tab of a sharing interface. It includes sections for 'Access Levels', 'Email Alert', and 'Email Addresses'. The 'Access Levels' section contains several checkboxes: 'Can Delete' (checked), 'Can Upload' (checked), 'Can Create Folder' (checked), 'Can Download File' (unchecked), 'Can Download Folder' (unchecked), 'Add Digital Signature' (unchecked), and 'View with Copy Protect' (unchecked). The 'Email Alert' section has checkboxes for 'Download' (checked), 'Delete' (checked), 'Upload' (checked), 'View' (unchecked), and 'Create Folder' (unchecked). The 'Email Addresses' section shows two entered addresses: 'Jim@outlook.com' and 'Sam@outlook.com'. At the bottom are 'CANCEL' and 'CREATE SHARE' buttons.

A storage request message

A content request message

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/> (annotated)

	<h2>Verification</h2> <ul style="list-style-type: none"> <li>• For verifying the above procedure pertaining to file sharing, Copy the <b>Shareable Link</b> from the shares.</li> <li>• Open the link in browser tab. This will redirect to Form based authentication.</li> <li>• Once the authentication is effective, you should be able to access <b>Shares</b> assigned to the login profile.</li> <li>• This link can be emailed or shared with your users.</li> </ul> <p>Source: <a href="https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/">https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/</a></p> <p>Further, to the extent this element is performed at least in part by Defendant’s software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.</p>
<p>[7.4] if the request message is the storage request message, then determining whether the requested media content is available for storage; and</p>	<p>Company performs and/or induces others to perform the step wherein if the request message is the storage request message, then determining whether the requested media content is available for storage.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Nirvashare enables file owners to share file through a URL with access-level permissions such as ‘view with copy protect’ or ‘can download folder’. Therefore, upon information and belief, when the user with whom the files are shared, requests to download a file, Nirvashare verifies the associated permissions to determine whether the file can be downloaded (“determining whether the requested media content is available for storage”) or if access is restricted to viewing only.</p>

## Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: <https://nirvashare.com/white-papers/>

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

the storage request message

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/> (annotated)

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

[7.5] if the request message is the content request message, then

Company performs and/or induces others to perform the step wherein if the request message is the content request message, then initiating delivery of the requested media content to the consumer device.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

initiating delivery of the requested media content to the consumer device;

For example, when the user with whom the files are shared requests to view them (“if the request message is the content request message”), the Nirvashare platform delivers the files by displaying them on the user’s device (“initiating delivery of the requested media content to the consumer device”).

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

if the request message is the content request message

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/> (annotated)



## Storing Objects in a Bucket

media content

You can store objects in a bucket in Wasabi. An object can be any type of file—text, photo, video, etc. See [Step 2 in Getting Started: Working with a Bucket](#).

Source: <https://docs.wasabi.com/docs/storing-objects-in-a-bucket> (annotated)

## Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: <https://nirvashare.com/white-papers/>

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

[7.6] wherein the media data includes time data that indicates a length of time to store the requested media content; and

Company performs and/or induces others to perform the step wherein the media data includes time data that indicates a length of time to store the requested media content.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

For example, Nirvashare enables file owners to share files with a predefined expiration period (“the media data includes time data”), ensuring that the shared files remain accessible for the duration set by the file owner. Once this period expires, access to the shared files is automatically revoked, preventing further downloads or viewing. Therefore, upon information and belief, the specified time frame in which the user (with whom the files are shared) can download the file indicates a length of time to store the requested media content.

Optionally, you can also set a specific duration for the share after which it becomes inactive by specifying the from and to dates in the duration tab.

The screenshot shows the 'CREATE NEW SHARE' interface in Nirvashare. The path is 'elasticbeanstalk-ap-south-1-100674486567/test folder/'. The 'Authentication' tab is selected, showing options: Public Access, Basic Authentication, Form based Authentication (selected), External Auth Provider, and OTP. A 'New' button is next to the 'Form 1' dropdown. The 'Duration' tab is also visible. At the bottom are 'Setup Guide 4', 'CREATE SHARE', and 'CANCEL' buttons.

Source: <https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi>

	<div data-bbox="409 256 1493 500" style="border: 2px solid red; padding: 10px;"> <h3>Duration</h3> <p>Start and end date can be specified for the <b>Share</b> validity period, which will make <b>Share</b> to be available only for the specified duration.</p> </div> <div data-bbox="426 548 1493 1036" style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; padding-bottom: 5px;"> <span>Basic Info</span> <span>Permissions</span> <span>Authentication</span> <span style="border-bottom: 2px solid #00aaff;">Duration</span> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="border: 2px solid red; padding: 5px; flex: 1;"> <p>From Date</p> <p>MM/DD/YYYY</p> </div> <div style="flex: 1; text-align: center;"> <p>📅</p> </div> <div style="border: 2px solid red; padding: 5px; flex: 1;"> <p>End Date</p> <p>MM/DD/YYYY</p> </div> <div style="flex: 1; text-align: center;"> <p>📅</p> </div> </div> <div style="display: flex; justify-content: flex-end; margin-top: 20px;"> <span style="background-color: #00aaff; color: white; padding: 5px 10px; border-radius: 5px;">CANCEL</span> <span style="background-color: #c8e6c9; color: #00aaff; padding: 5px 10px; border-radius: 5px; margin-left: 10px;">CREATE SHARE</span> </div> </div> <div data-bbox="1528 646 1837 714" style="color: red; margin-top: 20px;"> <p>the media data includes time data</p> </div> <p>Source: <a href="https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/">https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/</a></p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.</p>
<p>[7.7] the first processor is further configured to determine</p>	<p>Company performs and induces others to perform the step wherein the first processor is configured to determine whether the requested media content exists.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p>

whether the requested media content exists; and

For example, Nirvashare allows file owners to share files with a specified expiration period, ensuring that shared files and folders remain accessible for a set duration. Additionally, shared files are assigned access-level permissions such as ‘view with copy protect’ or ‘can download folder’. Therefore, it would be apparent to the person having ordinary skills in the art that Nirvashare utilizes a processor to determine whether the requested file has ‘view with copy protect’ access, ‘can download folder’ access, or if the file’s access period has expired (“the first processor is configured to determine whether the requested media content exists”).

### Duration

Start and end date can be specified for the **Share** validity period, which will make **Share** to be available only for the specified duration.

The screenshot shows a web interface for creating a share. At the top, there are four tabs: 'Basic Info', 'Permissions', 'Authentication', and 'Duration'. The 'Duration' tab is selected and highlighted with a red box. Below the tabs, there are two input fields: 'From Date' and 'End Date', both with calendar icons. These fields are also highlighted with a red box. At the bottom right, there are two buttons: 'CANCEL' (blue) and 'CREATE SHARE' (green).

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

The screenshot displays the 'Permissions' tab of a sharing interface. It features four main sections: 'Basic Info', 'Permissions' (active), 'Authentication', and 'Duration'. Under 'Access Levels', there are checkboxes for 'Can Delete' (checked), 'Can Upload' (checked), 'Can Create Folder' (checked), 'Can Download File' (unchecked), 'Can Download Folder' (unchecked), 'Add Digital Signature' (unchecked), and 'View with Copy Protect' (unchecked). The 'Email Alert' section includes checkboxes for 'Download' (checked), 'Delete' (checked), 'Upload' (checked), 'View' (unchecked), and 'Create Folder' (unchecked). Below these are two input fields for 'Email Addresses' containing 'Jim@outlook.com' and 'Sam@outlook.com'. At the bottom right are 'CANCEL' and 'CREATE SHARE' buttons.

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>

## Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: <https://nirvashare.com/white-papers/>

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

<p>[7.8] if the processor determines that the requested media content exists, the processor is further configured to determine whether the requested media content is available and whether there are restrictions associated with the requested media content that prevent the requested media content from being delivered to</p>	<p>Company performs and induces others to perform the step wherein, if the processor determines that the requested media content exists, the processor is further configured to determine whether the requested media content is available and whether there are restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Nirvashare allows file owners to apply access restrictions based on the user's IP address (“restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device”). Further, it enables the file owners to set restrictions such as to only view or both view and download the files. Therefore, it would be apparent to a person having ordinary skills in the art that Nirvashare utilizes the processor to determine whether the requested media content is available and whether there are restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device.</p>
---	--

the consumer device.

< All Topics

Main > Administrative Guide > Access Restriction with IP Address

## Access Restriction With IP Address

While sharing a file/folder with users, access can be restricted to certain white listed IP or a range of IP addresses. In this guide, we will walk you through on how to set the IP address.

### Login Profile

Access Restriction can be set in the Login Profile created in NirvaShare. When a user tries to access the Shares, the login will proceed only if the user originating client IP matches the one mentioned in Access Restriction. Below are the steps to set the IP Access Restriction.

- While creating or editing existing Login Profile, click on the Access tab, set the IP address in the text box of **IP Address Restriction**.
- The valid format is the single IP address or can be IP range in IPv4 format.
- For single IP, enter the IP address. Example *49.207.200.108*
- For an IP range, enter two IP range addresses. Example *49.207.200.100 – 49.207.200.120*
- For more than one IP, a range can be specified and each of them should be separated by a comma.

*Example 49.207.200.45, 49.105.100.12*

Source: <https://nirvashare.com/docs/administrative-guide/access-restriction-with-ip-address/>



## Access

- Provide an IP Address or IP Addresses in the IP Address Restriction field.
- Choose the language in the Language field. By default it is set to English.

Note - To restrict access to only certain white listed IP address or a range, please refer to [Access Restriction with IP Address](#)

The screenshot shows a web form with three tabs: 'Basic Info', 'Access', and 'Authentication'. The 'Access' tab is active. It contains two main sections: 'IP Address Restriction' and 'Language'. The 'IP Address Restriction' section has a text input field with the value '49.207.200.100 , 49.207.200.120'. The 'Language' section has a dropdown menu with 'English' selected. At the bottom right of the form are two buttons: 'CANCEL' and 'CREATE'.

restrictions associated with the requested media content that prevent the requested media content from being delivered to the consumer device

Source: <https://nirvashare.com/docs/administrative-guide/login-profiles/login-profile-form-based-authentication/> (annotated)

A fine level of access permission can be set here for a shared file or folder. You can also provide one or more email addresses to get notified whenever events such as a new file is uploaded, downloaded etc. Email addresses have to be separated by a comma.

The screenshot displays the 'Permissions' tab of a sharing interface. It includes sections for 'Access Levels' with various permission checkboxes, an 'Email Alert' section with checkboxes for different actions, and an 'Email Addresses' section with two pre-filled email addresses. The 'CREATE SHARE' button is highlighted in green.

Section	Item	Status
Access Levels	Can Delete	Checked
	Can Upload	Checked
	Can Create Folder	Checked
	Can Download File	Unchecked
	Can Download Folder	Unchecked
	Add Digital Signature	Unchecked
	View with Copy Protect	Unchecked
Email Alert	Download	Checked
	Delete	Checked
	Upload	Checked
	View	Unchecked
	Create Folder	Unchecked
Email Addresses	Jim@outlook.com	Added
	Sam@outlook.com	Added

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>

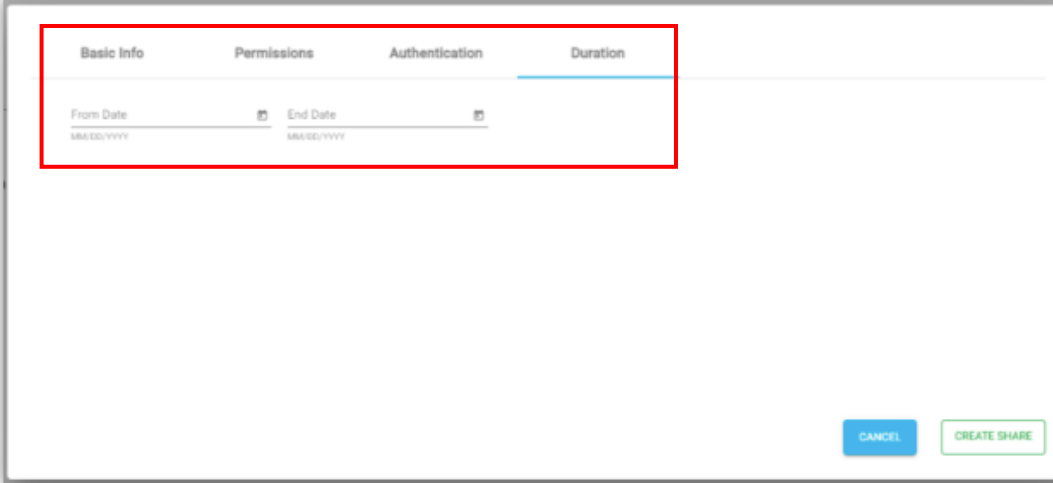
## Access Levels

Ability to share files with different access levels for different users. At times businesses may require to grant read only access to certain users and both read/write access to certain other users. With NirvaShare, fine access control can be given at file or folder level with a view, write, download, delete, etc operations. Besides, there can be multiple delegated admins and access to admins can also be moderated with role-based access control on the administrative tasks.

Source: <https://nirvashare.com/white-papers/>

## Duration

Start and end date can be specified for the **Share** validity period, which will make **Share** to be available only for the specified duration.



The screenshot shows a modal window for creating a share. It has four tabs: 'Basic Info', 'Permissions', 'Authentication', and 'Duration'. The 'Duration' tab is selected and highlighted with a blue underline. Inside this tab, there are two input fields: 'From Date' and 'End Date'. Both fields have a calendar icon to their right and a placeholder text 'MM/DD/YYYY'. A red rectangle highlights the 'Duration' tab and its input fields. At the bottom right of the modal, there are two buttons: 'CANCEL' (blue) and 'CREATE SHARE' (green).

Source: <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Company.

## 2. List of References

1. <https://wasabi.com/cloud-object-storage>, last accessed on 12 February 2025.
2. <https://docs.wasabi.com/v1/docs/wasabi-cloud-storage-console-1>, last accessed on 12 February 2025.
3. <https://nirvashare.com/>, last accessed on 12 February 2025.
4. <https://nirvashare.com/faqs/>, last accessed on 12 February 2025.
5. <https://docs.wasabi.com/docs/how-do-i-use-nirvashare-with-wasabi>, last accessed on 12 February 2025.
6. <https://docs.wasabi.com/docs/storing-objects-in-a-bucket>, last accessed on 12 February 2025.
7. [https://www.youtube.com/channel/UCP8znBILQ0b\\_2ixAak\\_iDcw](https://www.youtube.com/channel/UCP8znBILQ0b_2ixAak_iDcw), last accessed on 12 February 2025.
8. <https://nirvashare.com/how-to-share-file-folder-and-manage-access-to-wasabi-storage/>, last accessed on 12 February 2025.
9. <https://nirvashare.com/docs/administrative-guide/sharing-a-file-or-folder/>, last accessed on 12 February 2025.
10. <https://nirvashare.com/how-to-share-files-from-backblaze-b2-storage/>, last accessed on 12 February 2025.
11. <https://nirvashare.com/white-papers/>, last accessed on 12 February 2025.
12. <https://nirvashare.com/docs/administrative-guide/access-restriction-with-ip-address/>, last accessed on 12 February 2025.
13. <https://nirvashare.com/docs/administrative-guide/login-profiles/login-profile-form-based-authentication/>, last accessed on 12 February 2025.